

OFFICE OF THE CHIEF OF POLICE

SPECIAL ORDER NO. 23

July 16, 2007

APPROVED BY THE BOARD OF POLICE COMMISSIONERS ON JUNE 12, 2007

SUBJECT: ACCESS CONTROL POLICY FOR TEAMS II INFORMATION

PURPOSE: The Training Evaluation and Management System (TEAMS) application shall have the capability and shall operate in such a manner as to facilitate the following:

- * TEAMS information shall be provided to those with a "need to know" or "right to know" that information; and,
- * Access to TEAMS information pertaining to individual employees shall be restricted in a manner such that those who are not empowered via a "need to know" or "right to know" that information are prohibited from accessing such information.

PROCEDURE:

I. GUIDELINES. This access will be controlled by the following general guidelines:

- * All employees shall have the ability to view their own TEAMS Report;
- * All employees shall have the ability to view the event detail reports associated with the items on their TEAMS Report, but not such information as might compromise other security aspects of the system (e.g., complaint information pending an investigation);
- * All supervisors shall have the ability to view the TEAMS information pertaining to the employees who report to that supervisor or are otherwise in the supervisor's downward Chain of Command;
- * Managers and supervisors in an Area or organizational unit shall have the ability to view the TEAMS information for employees within their respective Area or organization, so long as those employees are of a rank below that of the manager or supervisor;
- * Employees assigned to Internal Affairs Group, Force Investigation Division, Use of Force Review Division, and Employee Relations Group (or their successor entities) shall have the ability to view all cases relevant to their particular type or area of

investigation and all TEAMS records pertaining to the employees involved in such cases;

- * Management may elect to restrict visibility to files of individuals assigned to undercover investigations or operations ("special assignment") for all Department employees. Such visibility shall not be restricted, however, from supervisors two levels up in the employee's Chain of Command;
- * The Chief of Police shall have the ability to view the TEAMS information for all Department employees, except those civilians working for the Police Commission or the Inspector General;
- * The Inspector General shall have the ability to view the TEAMS information for all Department employees;
- * Each member of the Board of Police Commissioners shall have the ability to view TEAMS information for all Department employees;
- * Assistant Chiefs, Deputy Chiefs, Commanders and Captains shall have the ability to view TEAMS information for Department employees outside of their Chain of Command, so long as those employees are of a rank below that of the Assistant Chief, Deputy Chief, Commander or Captain;
- * Managers and supervisors may delegate their access roles to their subordinates but shall remain responsible for any breaches of security;
- * Managers and supervisors may reassign the work of those in their downward Chain of Command to another individual, remove items from worklists of unavailable subordinates, and take other appropriate action to ensure the prompt completion of work items during periods of employee absence;
- * The TEAMS administrative staff shall be empowered to access the TEAMS information pertaining to all Department employees, revise individual employee access as consistent with these guidelines, or take such other actions as may be appropriate to administer the system; and,
- * For organizational units provided with "organizational worklists" within the TEAMS application, the Officer in Charge of each organization shall determine which organization employees shall have access to the worklist and the transactions sent thereto.

July 16, 2007

II. MISUSE OR ABUSE OF ACTION ITEM INFORMATION. Employees are reminded that any misuse or abuse of information contained within the Risk Management Information System (RMIS) or other TEAMS II Systems may result in disciplinary action. LAPD Manual Section 3/405 outlines the Department's policy regarding confidential files, documents, records and reports in the custody of Department employees. The unauthorized use of information obtained through employment with the Department can subject the employee to possible disciplinary action and/or criminal prosecution. This includes information obtained from manually stored records, as well as information obtained from automated records (e.g., RMIS).

AMENDMENTS: This Order amends Sections 1/668.02 and 1/668.06 of the Department Manual.

AUDIT RESPONSIBILITY: The Commanding Officer, Risk Management Group, shall monitor compliance with this directive in accordance with Department Manual Section 0/080.30.

WILLIAM J. BRATTON
Chief of Police

DISTRIBUTION "D"